UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK
MANHATTAN DIVISION

KEVIN VANDERMARK, individually and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

MASON TENDERS DISTRICT COUNCIL WELFARE FUND; MASON TENDERS DISTRICT COUNCIL PENSION FUND; MASON TENDERS DISTRICT COUNCIL ANNUITY FUND; and MASON TENDERS DISTRICT COUNCIL OF GREATER NEW YORK,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Kevin Vandermark (the "Plaintiff"), on behalf of himself and all others similarly situated, brings this Class Action Complaint (the "Action") and alleges against the above-captioned Defendants (collectively, the "Defendant" or "Mason Tenders") upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

I. NATURE OF THE ACTION

1. Plaintiff brings this Class Action Complaint (the "Action") against Mason Tenders, a labor organization in New York that has nearly 15,000 members including construction workers, hazardous materials handlers, recycling/waste handlers, and others.

2. On or about July 7, 2022, Mason Tenders posted or caused to be posted a notice entitled "Notice of Data Incident (hereinafter, the "Notice") announcing publicly that "unauthorized access to certain of the Funds' computer systems" occurred between December 2, 2021 and April 18, 2022 (hereinafter, the "Data Breach").[1] While hackers had unfettered access to these computer systems for nearly five months, Mason Tenders failed to adequately monitor their computer systems for intrusions and therefore did not discover the intrusion(s) for months after they initially occurred. To compound matters, the information taken in the Data Breach is highly sensitive and includes personally identifiable information ("PII"), including names, dates of birth, and Social Security numbers as well as protected health information ("PHI"), which includes medical information and health insurance information (collectively, and hereinafter, the "Private information").

3. As detailed below, this Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect

[1] https://member.mtdctrustfunds.org/PublicPages/Mason%20Tenders%20-%20Web%20Notice.pdf, (last accessed Aug. 1, 2022)("*Notice*").

Plaintiff Vandermark's and the Class Members' Private Information despite the fact that data breach attacks are at an all-time high.

4. Defendant's failure to enact reasonable safeguards enabled an unauthorized third-party to access Defendant's computer systems and the highly sensitive and confidential data of over 20,000 victims who entrusted their Private Information to Mason Tenders. Indeed, Plaintiff received the Notice from Defendant informing him that the information accessed by third-party actors included his Private Information.

5. Defendant omits key information from its Notice letters, including the Notice letter sent to Plaintiff, such as: (1) how the unauthorized intrusion occurred, (2) why Defendant waited from April 17, 2022 (when it first became cognizant of the Data Breach) until July 7, 2022 to post a notice informing victims that their information had been compromised, and (3) what remedial measures Defendant was taking to protect the data that Defendant continues to maintain to date.

6. Defendant has not offered Plaintiff and the Class Members any sort of real relief for the harm caused by the Data Breach. Defendant has only offered Plaintiff and the Class 1 year of credit monitoring, which is woefully insufficient given that the types of information stolen in this Data Breach could have lasting implications for Plaintiff and Class Members for years to come.

7. As a consequence of the Data Breach, Plaintiff's and Class Members' Private Information has been released into the public domain and they have had to, and will continue to have to, spend time to protect themselves from fraud and identity theft or to mitigate successful attempts at fraud or identity theft.

8. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to

Defendant, through frequent news reports and government warnings, and thus it was on notice that failing to take steps necessary to secure the Private Information from those risks left the property in a dangerous and vulnerable condition.

9. Defendant disregarded the rights of Plaintiff and Class Members by, inter alia, intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach and failing to provide Plaintiff and Class Members accurate notice of the Data Breach.

10. Plaintiff's and Class Members' identities are now at risk due to Defendant's conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

13. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, all forms of allowable damages, including statutory damages, compensatory damages, nominal damages, reimbursement

of out-of-pocket costs; injunctive relief including improvements to Defendant's data security systems, future annual audits; and adequate credit monitoring services funded by Defendant.

II. JURISDICTION AND VENUE

15. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member from the putative Class is from a different state than the Defendant (who is located in New York).

16. The Southern District of New York has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and conducts substantial business in New York and this District through its headquarters, offices, and affiliates.

17. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and has caused harm to Class Members residing in this District.

III. PARTIES

Plaintiff Kevin Vandermark

18. Plaintiff Kevin Vandermark is a member of Defendant's labor organization and is a resident and citizen of the state of New York. Plaintiff received the Notice on July 7, 2022. Plaintiff was informed in the Notice that his Private Information was compromised in the Data Breach.

The Mason Tenders Defendants

19. Defendant Mason Tenders is a New York-based labor organization, as defined by the Taft-Hartley Act, which serves employees in the construction and labor industry throughout the Greater New York-area.[2]

20. The Mason Tenders Defendants are Mason Tenders District Council Welfare Fund, Mason Tenders District Council Pension Fund, Mason Tenders District Council Annuity Fund and Mason Tenders District Council of Greater New York. Upon information and belief, Mason Tenders District Council of Greater New York is associated with, provides governance to, oversees, or controls in some manner the three funds that were implicated in this Data Breach, the welfare, pension, and annuity funds – which are represented by Defendants Mason Tenders District Council Welfare Fund, Mason Tenders District Council Pension Fund, Mason Tenders District Council Annuity Fund.

21. The Mason Tenders defendants maintain their principal place of business at 520 Eighth Avenue, Suite 600, New York, New York 10018.

IV. FACTUAL ALLEGATIONS

Defendant's Business

22. Defendant Mason Tenders District Council of Greater New York is a union defined as a labor organization within the meaning of the Taft-Hartley Act and represents employees in an industry affecting commerce as defined by the Taft-Hartley Act.[3]

23. Defendant's funds (the Welfare, Pension and Annuity Funds) provide welfare, retirement, training, and other benefits to eligible employees on whose behalf employers in the

[2] *See Mason Tenders District Council Welfare Fund, et al. v. Steel Construction LLC, et al.* Case No. 1:22-cv-06312 (S.D.N.Y., filed July 25, 2022), at ECF No. 1.
[3] *Id.*

construction industry contribute to the Funds pursuant to collective bargaining agreements made between such employers and the Mason Tenders District Council of Greater New York.[4]

24. Upon information and belief, in the ordinary course of doing business with the Defendant, victims of the Data Breach were required to provide, at a minimum, the Private Information – which is the information set compromised in this Data Breach, i.e., names, dates of birth, Social Security numbers, medical information and health insurance information.

25. Plaintiff and Class Members were required to and did in fact turn over and entrust to Defendant the private and confidential information listed above. Indeed, as a condition of receiving services from Defendant, Plaintiff and the Class Members were required entrust the Private Information at Defendant's request.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

27. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

28. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

The Data Breach

29. On or about July 7, 2022, Defendant began noticing the victims of the Data Breach. As the Notice states:

---

[4] *Id.*

> On April 17, 2022, the Funds became aware of suspicious activity related to certain of the Funds' computer systems. The Funds immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The Funds' investigation determined that there was unauthorized access to certain of the Funds' computer systems between December 2, 2021 to April 18, 2022. While on the network, the unauthorized actor had the ability to access certain directories stored therein. Therefore, the Funds undertook a comprehensive review of the contents of the directories to determine what, if any, sensitive information was contained within them and to whom the information related. On June 14, 2022, the Funds' review determined that the directories contained certain information related to some of the individuals who participate in and receive benefits from the Funds.[5]

30. The Notice then details the aforementioned Private Information as the information that "may" have been affected.

31. Although the Notice states that an unauthorized attacker first gained access to Defendant's network beginning December 2, 2021, the scope of the attack is unclear because the Notice provides scant detail about the nature or severity of the attack. Even worse, Defendant did not cause the Notice to be posted on its website until months after Defendant first became aware of the Data Breach on April 17, 2022. Defendant's Notice also evidences the fact that the Defendant allowed the "unauthorized actors" to roam freely in their computer systems for months before Defendant detected the unauthorized access and finally removed the attacker from being able to access Defendant's systems.

32. But what is clear from the Notice is that cybercriminals did, in fact, access and view Plaintiff's and Class members' PII and PHI during the four months in which the cybercriminals had unfettered access to Defendant's IT network.

33. Simply put, Defendant could have and should have prevented this Data Breach but Defendant did not implement or maintain adequate measures to protect its patients' PII and PHI.

---

[5] *Notice.*

34. On information and belief, the PII and PHI compromised in the files accessed by hackers was not encrypted. If the information were properly encrypted, the attacker would not have been able to exfiltrate intelligible data.

35. Due to Defendant's incompetent security measures, Plaintiff and the Class Members now face a present and substantial risk of fraud and identity theft and must deal with that threat for the remainder of their lives.

36. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII and PHI, Defendant provided unreasonably deficient data security prior to and throughout the Data Breach, including, but not limited to a lack of security measures for storing and handling patients' PII and PHI and inadequate employee training regarding how to access, handle and safeguard this information.

37. Defendant failed to adequately adopt and train its employees on even the most basic of information security protocols, including: storing, locking encrypting and limiting access to highly sensitive PHI and PII; implementing guidelines for accessing, maintaining and communicating sensitive PHI and PII, and protecting Plaintiff's and Class Members' sensitive PHI and PII by implementing protocols on how to utilize such information.

38. Defendant's failures caused the unpermitted disclosure of Plaintiff's and Class members' Private Information to an unauthorized third party and put Plaintiff and the Class at serious, immediate, and continuous risk of identity theft and fraud.

39. The Data Breach that exposed Plaintiff's and Class members' Private Information was caused by Defendant's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

40. Defendant failed to comply with security standards or to implement security measures that could have prevented or mitigated the harm resulting from the Data Breach.

41. Defendant failed to ensure that all personnel with access to Plaintiff's and Class Members' PII and PHI were properly trained in retrieving, handling, using and distributing sensitive information.

The Breach Was Foreseeable

42. Defendant had obligations created by HIPAA, industry standards, common law and contract law made to Plaintiff and Class Members to keep their PII and PHI confidential and to protect it from unauthorized access and disclosure.

43. Plaintiff and Class members provided their PII and PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

44. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

45. In 2021 alone there were over 220 data breach incidents.

46. These approximately 220 data breach incidents have impacted nearly 15 million individuals.

47. PII and PHI is of great value to hackers and cybercriminals, and the data compromised in the Breach can be used in a variety of unlawful manners.

48. PII and PHI can be used to distinguish, identify, or trace an individual's identity, such as their name and medical records.

49. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

50. Given the nature of this Data Breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cybercriminals in a variety of different ways.

51. Indeed, the cybercriminals who possess the Class members' PII and PHI, especially their Social Security numbers (as here), can readily obtain Class members' tax returns or open fraudulent credit card accounts in the Class members' names.

52. Because the increase in frequency and severity of cyber attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, Defendant knew or should have known of its duty to safeguard the Private Information and the consequences of its failure to do so.

Defendant Failed to Follow FTC Guidelines

53. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

54. According to the FTC, the need for data security should be factored into all business decision-making.

55. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

56. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

57. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

58. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. Defendant failed to properly implement basic data security practices.

61. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

62. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Meet Industry Standards

63. Several best practices have been identified that a minimum should be implemented by an entity like Defendant, including but not limited to: educating all employees and implementing strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

64. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

65. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

66. These foregoing frameworks are existing and applicable industry standards in the industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Breach.

Defendant Failed to Comply with HIPAA

67. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

68. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

69. Title II of HIPAA contains what are known as the Administrative Simplification provisions. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI and PII like the data Defendant left unguarded.

70. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D) and 45 C.F.R. § 164.530(b).

> A data breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

71. Data breaches are Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).

72. Defendant's Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

Defendants' Breach

73. Defendant breached its obligations to Plaintiff and the Class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, network and data.

74. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect PHI and other PII and PHI;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene; Failing to avoid the use of domain-wide, admin-level service accounts;

g. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

h. Failing to properly train and supervise employees in the proper handling of inbound emails;

i. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

j. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

k. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

l. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

m. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

n. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

o. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

p. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b) and/or;

q. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key," 45 CFR § 164.304 (definition of encryption).

75. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and the Class members' PII and PHI.

76. Accordingly, as outlined below, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud and identity theft.

Data Breaches Are Disruptive and Harmful

77. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

78. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

79. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

80. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number.

81. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

82. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

83. Theft of PII and PHI is gravely serious. PII and PHI is an extremely valuable property right.

84. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII and PHI has considerable market value.

85. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[14]

86. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose

of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

87. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when PII, PHI, and/or financial information is stolen and when it is used.

88. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. See GAO Report, at p. 29.

89. PII and PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

90. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

91. Thus, Plaintiff and Class members must vigilantly monitor their financial and medical accounts for many years to come.

92. Sensitive PII and PHI can sell for as much as $363 per record according to the Infosec Institute.

93. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

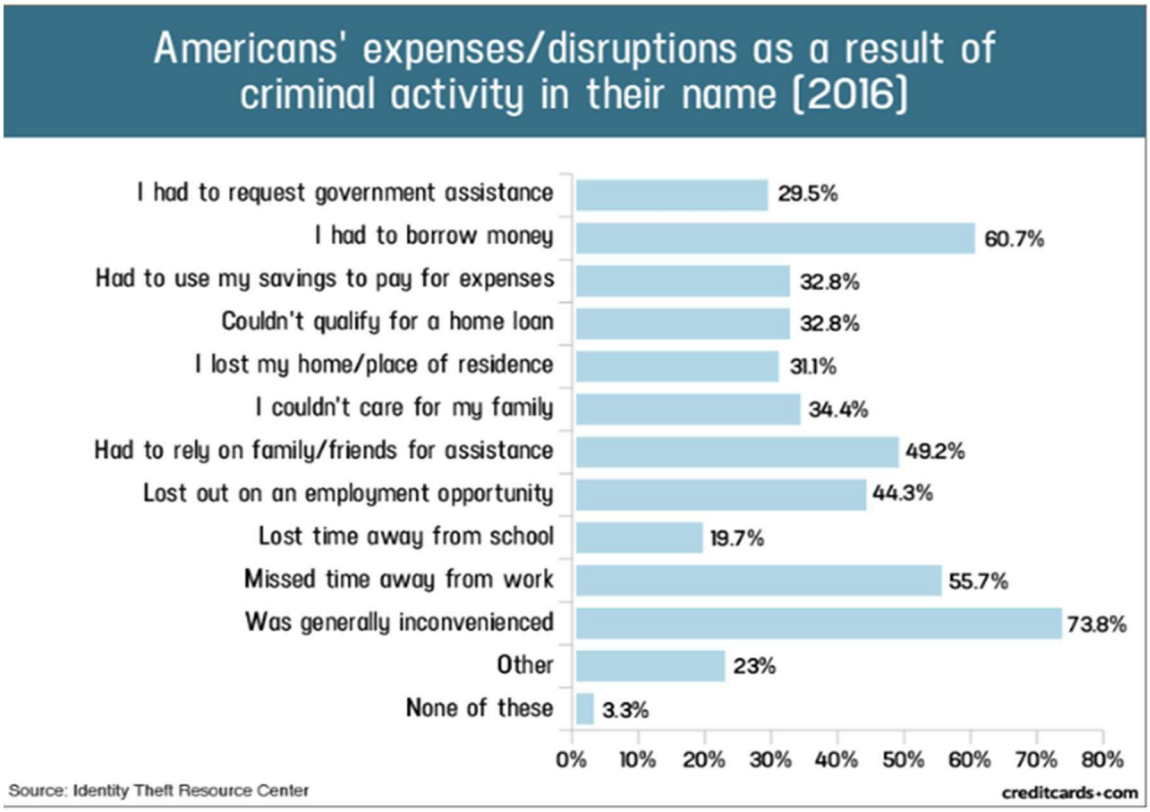
94. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

95. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

96. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

97. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[6]

[6] *See* Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. (last visited Jan. 25, 2022).



98. Additionally, Medical information is especially valuable to identity thieves.

99. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.

100. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

101. For this reason, Defendant knew or should have known about these dangers and strengthened its network and data security systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Harm to Plaintiff

102. On or about July 7, 2022 Plaintiff received a Notice letter from Defendant that his Private Information had been improperly accessed and/or obtained by unauthorized third parties.

The Notice indicated that Plaintiff's Private Information was compromised as a result of the Data Breach.

103. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has spent several hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

104. As a result of the Data Breach, Plaintiff has suffered theft attempts due to the exposure of his Private Information, including unauthorized charges on one of his credit/debit cards.

105. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

106. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

107. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a

result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

108. This Action is properly maintainable as a Class Action.

109. Plaintiff brings this Action on behalf of himself and all similarly situated persons and entities pursuant to Federal Rule of Civil Procedure 23, for the following Class defined as:

> All individuals and entities residing in the United States whose Private Information was compromised on the Data Breach announced by the Defendant in July of 2022 (the "Class").

110. Excluded from the Class are: Defendant and Defendant's relatives, subsidiaries, affiliates, officers and directors, and any entity in which the Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

111. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

112. Numerosity. Defendant reports that the Data Breach compromised the Private Information of over 20,000 victims. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

113. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner and

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, equitable relief and/or injunctive relief.

114. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's Private Information, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by Defendant's uniform conduct. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and

those of other Class members arise from the same operative facts and are based on the same legal theories.

115. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class in that he has no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel experienced in complex consumer class action litigation, including, but not limited to, similar data breach class action litigation, and Plaintiff intends to prosecute this action vigorously.

116. Superiority of Class Action. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

117. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

118. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

119. Predominance. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

120. This proposed class action does not present any unique management difficulties.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

NEGLIGENCE

121. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

122. Plaintiff brings this cause of action on behalf of himself and the Class.

123. Defendant required Plaintiff and the Class Members to submit non-public personal information in order to obtain services.

124. The Class members are individuals who provided certain PII and PHI to Defendant including the Private Information described above.

125. Defendant had full knowledge of the sensitivity of the PII and PHI to which it was entrusted and the types of harm that Class members could and would suffer if the information were wrongfully disclosed.

126. Defendant had a duty to each Class member to exercise reasonable care in holding, safeguarding and protecting that information.

127. Plaintiff and the Class members were the foreseeable victims of any inadequate safety and security practices.

128. The Class members had no ability to protect their data in Defendant’s exclusive control and possession.

129. By collecting and storing this data in its computer property, and by sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and the Class members' PII and PHI held within it — to prevent disclosure of the information and to safeguard the information from theft.

130. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

131. Defendant owed a duty of care to safeguard the PII and PHI of Plaintiff and Class Members in its custody. This duty of care arises because Defendant knew of a foreseeable risk to the data security systems it used. Defendant knew of this foreseeable risk because of the explosion of ransomware and data breach incidents involving healthcare providers detailed above. Despite its knowledge of this foreseeable risk, Defendant failed to implement reasonable security measures.

132. Defendant owed a duty of care to Plaintiff and the Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII and PHI.

133. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as the common law.

134. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

135. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

136. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

137. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

138. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

139. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Class members' PHI and PII.

140. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures to safeguard Class members' PII and PHI;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class members' PII and PHI;

e. Failing to detect in a timely manner that Class members' PII and PHI had been compromised;

f. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages and

g. Failing to have mitigation and back-up plans in place in the event of a cyber- attack and data breach.

141. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII and PHI would result in injury to Plaintiff and Class members.

142. Further, the breach of security was reasonably foreseeable given the known high frequency of hacking incidents, cyberattacks, and data breaches in the healthcare industry.

143. It was therefore foreseeable that the failure to adequately safeguard Class members' PII and PHI would result in one or more types of injuries to Class members.

144. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Breach.

145. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) provide adequate credit monitoring to all Class members.

SECOND CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

146. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

147. Plaintiff brings this cause of action on behalf of himself and the Class.

148. Defendant acquired and maintained the Private Information of Plaintiff and the Class as a condition of their receiving services from Defendant.

149. At the time Defendant acquired the PII and PHI of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the Private Information and not take unjustified risks when storing the Private Information.

150. Plaintiff and the Class would not have entrusted their Private Information to Defendant had they known that Defendant would make the Private Information internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII and PHI that Defendant no longer had a reasonable need to maintain.

151. Defendant further promised to comply with industry standards and to ensure that Plaintiff's and Class Members' PII and PHI would remain protected.

152. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

153. In collecting and maintaining the Private Information of Plaintiff and the Class, Defendant entered into contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PII and PHI of Plaintiff and the Class.

154. Plaintiff and the Class fully performed their obligations under the contracts with Defendant.

155. Defendant breached the contracts they made with Plaintiff and the Class by failing to protect and keep private financial information of Plaintiff and the Class, including failing to (i) encrypt or tokenize the sensitive Private Information of Plaintiff and the Class, (ii) delete such Private Information that Defendant no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such Private Information.

156. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

157. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class Members are at an increased risk of identity theft or fraud.

158. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class Members are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

THIRD CAUSE OF ACTION

UNJUST ENRICHMENT

159. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

160. Plaintiff brings this cause of action in the alternative to Count II, Breach of Implied Contract.

161. Plaintiff brings this cause of action on behalf of himself and the Class.

162. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of fees paid. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

163. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

164. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

165. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed

to implement appropriate data management and security measures that are mandated by industry standards.

166. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

167. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

168. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

169. Plaintiff and Class Members have no adequate remedy at law.

170. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended

to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

171. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

172. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

VII. PRAYER FOR RELIEF

173. WHEREFORE, Plaintiff, on his own and behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiff and his counsel to represent the Class;

B. For an award of actual damages, compensatory damages, nominal damages and statutory penalties, in an amount to be determined, as allowable by law;

C. For an award of damages, equitable, and injunctive relief, as well as reasonable attorneys' fees and costs.

D. For an award of punitive damages, as allowable by law;

E. For injunctive and other equitable relief to ensure the protection of the Private Information of Plaintiff and the Class which remains in Defendant's possession.

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as the Court may deem just and proper.

VIII. JURY TRIAL DEMAND

Plaintiff hereby demands a jury trial of all claims to triable.

DATED: Aug. 11, 2022

Respectfully submitted,

s/ Blake Hunter Yagman

Blake Hunter Yagman
byagman@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (212) 594-5300

Gary M. Klinger*
gklinger@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street
Suite 2100
Chicago, IL 60606
Tel.: (866) 252-0878

ATTORNEYS FOR PLAINTIFF

**Pro Hac Vice Forthcoming*